Claims

WE CLAIM:

1. A method for generating a permission grant set for a code assembly received from a resource location, the method comprising:

receiving a security policy specification defining a plurality of code groups, each code group being associated with a code-group permission set;

receiving evidence associated with the code assembly;

evaluating the evidence relative to the code groups to determine membership of the code assembly in one or more of the code groups; and

generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is a member.

2. The method of claim 1 wherein the generating operation comprises:

dynamically generating a code-group permission set based on permissions associated with the one or more code groups.

3. The method of claim 1 wherein the generating operation comprises:

computing a logical set operation on code-group permission sets associated with the code groups in which the code assembly is a member to generate the permission grant set.

4. The method of claim 3 wherein the computing operation comprises:

computing the logical set operation based on order values associated with the code

groups.

5. The method of claim 1 wherein the generating operation comprises:

computing a union of the code-group permission sets associated with code groups in which the code assembly is a member to generate the permission grant set.

6. The method of claim 1 wherein the security policy specification further defines at least one code group collection associated with the plurality of code groups and the generating operation comprises:

selecting a code-group permission set associated with an individual code group of the code group collection in which the code assembly is a member to generate the permission grant set.

7. The method of claim 6 wherein the security policy specification defines the at least one code group collection as a code group hierarchy.

8. The method of claim 6 further comprising:

an exclusive property associated with the single code group indicating that the code-group permission set associated with the single code group is to be selected to generate the permission grant set.

9. The method of claim 8 further comprising:

an exclusive property associated with the single code group indicating that no code-group permission set associated with a code group existing below the single code group in a code group hierarchy is to be used to generate the permission grant set.

10. The method of claim 1 wherein the security policy specification further defines a policy level associated with the plurality of code groups, and the generating operation comprises:

computing a union of the code-group permission sets associated with code groups in which the code assembly is a member to generate a policy-level permission set; and

generating the permission grant set based on the policy-level permission set.

11. The method of claim 1 wherein the security policy specification further defines at least one code group collection associated with the plurality of code groups and a policy level associated with the at least one code group collection, and the generating operation comprises:

selecting a code-group permission set associated with an individual code group of the code group collection in which the code assembly is a member to generate a policy-level permission set; and

generating the permission grant set based on the policy-level permission set.

12. The method of claim 1 wherein the security policy specification further defines a plurality of policy levels, each policy level being associated with the plurality of code groups, and the generating operation comprises:

selecting, for each policy level, a code-group permission set associated with an individual code group in the code groups of the policy level in which the code assembly is a member to generate a corresponding policy-level permission set; and

merging the corresponding policy-level permission sets to generate the permission grant set.

13. The method of claim 12 wherein the merging operation comprises:

computing an intersection of the corresponding policy-level permission sets associated with each policy level.

14. The method of claim 1 wherein the security policy specification further defines a plurality of policy levels, each policy level being associated with a plurality of code groups, and the generating operation comprises:

computing, for each policy level, a union of the code-group permission sets associated with code groups of the policy level in which the code assembly is a member to generate a corresponding policy-level permission set; and

merging the corresponding policy-level permission sets to generate the permission grant set.

15. The method of claim 14 wherein the merging operation comprises:

computing an intersection of the corresponding policy-level permission sets associated with each policy level.

16. The method of claim 1 wherein the security policy specification further defines a plurality of ordered policy levels associated with the plurality of code groups, such that a first policy level defines a more restrictive security policy than a second policy level.

17. The method of claim 1 further comprising:

extracting from the security policy specification a membership criterion for a code group in the plurality of code groups.

18. The method of claim 17 wherein the evaluating operation comprises:

extracting one or more trust characteristics from the evidence;

evaluating the trust characteristics relative to the membership criterion; and

identifying the code assembly as a member of the code group, if the one or more trust characteristics satisfy the membership criterion.

19. The method of claim 1 further comprising:

extracting from the security policy specification a code-group permission set for each code group in the plurality of code groups.

20. The method of claim 1 wherein the security policy specification further describes at least one code group hierarchy associated with the plurality of code groups, each code group collection including a parent code group, and further comprising:

extracting from the security policy specification a definition of at least one child code group of the parent code group in the at least one code group collection.

21. The method of claim 20 wherein the evaluating operation comprises:

determining whether the code assembly is a member of the parent code group; and

determining whether the code assembly is a member of the at least one child code group, if the code assembly is a member of the parent code group.

22. A method of claim 1 further comprising:

performing verification on the code assembly;

detecting a verification failure of the code assembly in the operation of performing

verification; and

determining based on the permission grant set whether the code assembly may be executed despite the verification failure.

23. A method of claim 1 further comprising:

determining based on the permission grant set that a step of a verification process is unnecessary;

communicating to a verification module that the step of the verification process may be bypassed;

performing the verification process on the code assembly with the verification module; and

bypassing the step of the verification process, responsive to the communicating operation.

24. A computer data signal embodied in a carrier wave by a computing system and encoding a computer program for executing a computer process generating a permission grant set for a code assembly received from a resource location, the computer process comprising:

receiving a security policy specification defining a plurality of code groups, each code group being associated with a code-group permission set;

receiving evidence associated with the code assembly;

evaluating the evidence relative to the code groups to determine membership of the code assembly in one or more of the code groups; and

generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is a member.

25. A computer program storage medium readable by a computer system and encoding a computer program for executing a computer process generating a permission grant set for a code assembly received from a resource location, the computer process comprising:

receiving a security policy specification defining a plurality of code groups, each code group being associated with a code-group permission set;

receiving evidence associated with the code assembly;

evaluating the evidence relative to the code groups to determine membership of the code assembly in one or more of the code groups; and

generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is a member.

26. A policy manager for generating a permission grant set for a code assembly received from a resource location, the code assembly being associated with an evidence set, the policy manager comprising:

a code group collection generator creating at least one code group collection in accordance with a definition specified in a security policy specification, each code group collection having a plurality of code groups, each code group being associated with a code-group permission set;

a membership evaluator determining membership of the code assembly in one or more code groups of the at least one code group collection based on the evidence set;

a permission set generator generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is determined to be a member.

27. The policy manager of claim 26 further comprising:

a parser reading the security policy specification and generating the definition of the at least one code group collection.

28. The policy manager of claim 26 wherein the permission set generator comprises:

a code-group permission set selector selecting a code-group permission set of an individual code group of the code group collection in which the code assembly is a member to generate the permission grant set.

29. The policy manager of claim 26 wherein the permission set generator comprises:

a code-group permission set merger computing a logical set operation of the code-group permission sets associated with code groups in which the code assembly is a member to generate the permission grant set.

30. The policy manager of claim 29 wherein the logical set operation is based on an order associated with each code group.

31. The policy manager of claim 26 wherein the permission set generator comprises:

a code-group permission set merger computing a union of the code-group permission sets associated with code groups in which the code assembly is a member to generate the permission grant set.

32. The policy manager of claim 26 wherein the code group collection generator generates a plurality of policy levels specified in the security policy specification, each policy level being associated with a code group collection, and the permission set generator comprises:

a code-group permission set generator generating a plurality of policy-level permission sets based on the one or more code-group permission sets; and

a policy-level permission set generator coupled to receive the plurality of policy-level permission sets from the code-group permission set generator to generate the permission grant set based on the policy-level permission sets.

33. The policy manager of claim 32 wherein the code-group permission set generator comprises:

a code-group permission set selector selecting a code-group permission set associated with an individual code group of the code group collection in which the code assembly is a member to generate the policy-level permission set.

34. The policy manager of claim 32 wherein the code-group permission set generator comprises:

a code-group permission set merger computing a union of the code-group permission sets associated with code groups in which the code assembly is a member to generate the policy-level permission set.

35. The policy manager of claim 32 wherein the policy-level permission set generator comprises:

a policy-level permission set merger merging the policy-level permission sets received from the code-group permission set generator to generate the permission grant set.

36. The policy manager of claim 35 wherein the policy-level permission set merger computes an intersection of the policy-level permission sets associated with each policy level.

37. A computer program product encoding a computer program for executing on a computer system a computer process for generating a permission grant set for a code assembly received from a resource location, the code assembly being associated with an evidence set, the computer process comprising:

receiving a security policy specification defining at least one code group collection having one or more code groups, each code group being associated with a code-group permission set;

evaluating the evidence set relative to the code group collection to determine membership of the code assembly in one or more code groups of the code group collection; and

generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is a member.

38. The program product of claim 37 wherein the generating operation comprises:

computing a union of the code-group permission sets associated with code groups of the code group collection in which the code assembly is a member to generate the permission grant set.

39. The program product of claim 37 wherein the generating operation comprises:

selecting a code-group permission set associated with an individual code group of the code group collection in which the code assembly is a member to generate the permission grant set.

40. The program product of claim 37 wherein the security policy specification further

defines a plurality of policy levels associated with the one or more code groups, and the generating operation comprises:

computing, for each policy level, a union of the code-group permission sets associated with code groups in which the code assembly is a member to generate a corresponding policy-level permission set; and

generating the permission grant set based on the corresponding policy-level permission set of each policy level.

41. The program product of claim 40 wherein the operation of generating the permission grant set based on one or more code-group permission sets further comprises:

computing an intersection of the corresponding policy-level permission sets associated with each policy level.

42. The program product of claim 40 wherein the operation of generating the permission grant set based on one or more code-group permission sets further comprises:

computing an intersection of a subset of the corresponding policy-level permission sets.

43. The program product of claim 37 wherein the computer process further comprises:

extracting from the security policy specification a membership criterion for a code group in the plurality of code groups.

44. The program product of claim 43 wherein the evaluating operation comprises:

extracting one or more trust characteristics from the evidence;

evaluating the trust characteristics relative to the membership criterion; and

identifying the code assembly as a member of the code group, if the trust characteristics satisfy the membership criterion.

45. The program product of claim 37, wherein the computer process further comprises:

caching the permission grant set in association with the evidence; and

outputting the permission grant set in response to a subsequent reciept of the evidence without re-evaluating the evidence.

46. A computer system providing security management relating to a code assembly received from a resource location, the code assembly being associated with evidence, the system comprising:

a policy manager evaluating the evidence relative to one or more code groups configured in at least one code group collection defined by a security policy specification to generate a permission grant set;

a run-time call stack associating the permission grant set with the code assembly; and

a virtual machine executing the code assembly to perform an operation, if the permission grant set satisfies permission requirements associated with the operation.

47. The computer system of claim 46 wherein the policy manager comprises:

a membership evaluator evaluating the evidence relative to the code group collection to determine membership of the code assembly in one or more code groups of the code group collection.

48. The computer system of claim 47 wherein the policy manager further comprises:

a permission set generator generating the permission grant set based on one or more code-group permission sets, each of the one or more code-group permission sets being associated with a code group in which the code assembly is a member.

49. A method of verifying a code assembly received from a resource location, the method comprising:

receiving a security policy specification defining a security policy;

receiving evidence associated with the code assembly;

evaluating the evidence relative to the security policy;

performing verification on the code assembly;

detecting a verification failure of the code assembly in the operation of performing verification; and

determining whether the code assembly may be executed despite the verification failure, responsive to the evaluating operation.

50. The method of claim 49 wherein the operation of receiving evidence comprises:

receiving evidence associated with a class of the code assembly.

51. The method of claim 49 wherein the operation of receiving evidence comprises:

receiving evidence associated with a module of the code assembly.

52. The method of claim 49 wherein the operation of receiving evidence comprises:

receiving evidence associated with a method of the code assembly.

53. A method of verifying a code assembly received from a resource location, the method comprising:

receiving a security policy specification defining a security policy;

receiving evidence associated with the code assembly;

evaluating the evidence relative to the security policy;

generating a permission grant set, responsive to the evaluating operation,

determining based on the permission grant set that a step of a verification process is unnecessary;

communicating to a verification module that the step of the verification process may be bypassed;

performing the verification process on the code assembly with the verification module; and

bypassing the step of the verification process, responsive to the communicating operation.

54. The method of claim 53 wherein the generating operation comprises:

generating the permission grant set in association with a module of the code assembly, responsive to the evaluating operation.

55. The method of claim 53 wherein the generating operation comprises:

generating the permission grant set in association with a class of the code assembly, responsive to the evaluating operation.

56. The method of claim 53 wherein the generating operation comprises:

generating the permission grant set in association with a method of the code assembly, responsive to the evaluating operation.